[perl #130635] [PATCH] Stack overflow in Storable retrieve_hook

Thread Previous

From:
John Lightsey

Date:
January 24, 2017 19:22
Subject:
[perl #130635] [PATCH] Stack overflow in Storable retrieve_hook
Message ID:
rt-4.0.24-26879-1485285748-923.130635-75-0@perl.org

```
# New Ticket Created by  John Lightsey
# Please include the string:  [perl #130635]
# in the subject line of all future correspondence about this issue.
# <URL: https://rt.perl.org/Ticket/Display.html?id=130635 >


This is a bug report for perl from john@nixnuts.net,
generated with the help of perlbug 1.40 running under perl 5.25.9.


-----------------------------------------------------------------
AFL detected a stack overflow in Storable's retrieve_hook() function.

The problem essentially is that a hook's classname length is read into
a signed integer, compared to the size of a stack buffer, then used to
read the classname. The size comparison treats the length as signed,
while the read treats the length as unsigned.

[Please do not change anything below this line]
-----------------------------------------------------------------
---
Flags:
    category=library
    severity=low
    Type=Patch
    PatchStatus=HasPatch
    module=Storable
---
Site configuration information for perl 5.25.9:

Configured by jd at Wed Jan  4 22:24:39 CST 2017.

Summary of my perl5 (revision 5 version 25 subversion 9) configuration:
  Snapshot of: 1e67156061b1f7aa186cda226e8470dfa1c5a681
  Platform:
    osname=linux
    osvers=4.8.0-2-amd64
    archname=x86_64-linux
    uname='linux slug 4.8.0-2-amd64 #1 smp debian 4.8.11-1 (2016-12-02) x86_64 gnulinux '
    config_args='-de -Dprefix=/home/jd/perl5/perlbrew/perls/perl-blead-new -Dcc=/usr/bin/afl-gcc -DDEBUGGING -Dusedevel -Aeval:scriptdir=/hom
    hint=recommended
    useposix=true
    d_sigaction=define
    useithreads=undef
    usemultiplicity=undef
    use64bitint=define
    use64bitall=define
    uselongdouble=undef
    usemymalloc=n
    bincompat5005=undef
  Compiler:
    cc='/usr/bin/afl-gcc'
    ccflags ='-fwrapv -DDEBUGGING -fno-strict-aliasing -pipe -fstack-protector-strong -I/usr/local/include -D_LARGEFILE_SOURCE -D_FILE_OFFSET
    optimize='-O2 -g'
    cppflags='-fwrapv -DDEBUGGING -fno-strict-aliasing -pipe -fstack-protector-strong -I/usr/local/include'
    ccversion=''
    gccversion='6.3.0 20161229'
    gccosandvers=''
    intsize=4
    longsize=8
    ptrsize=8
    doublesize=8
    byteorder=12345678
    doublekind=3
    d_longlong=define
    longlongsize=8
    d_longdbl=define
    longdblsize=16
    longdblkind=3
    ivtype='long'
    ivsize=8
    nvtype='double'
    nvsize=8
    Off_t='off_t'
    lseeksize=8
    alignbytes=8
    prototype=define
  Linker and Libraries:
    ld='/usr/bin/afl-gcc'
    ldflags =' -fstack-protector-strong -L/usr/local/lib'
```

```
    libpth=/usr/local/lib /usr/lib/gcc/x86_64-linux-gnu/6/include-fixed /usr/include/x86_64-linux-gnu /usr/lib /lib/x86_64-linux-gnu /lib/../
    libs=-lpthread -lnsl -ldl -lm -lcrypt -lutil -lc
    perllibs=-lpthread -lnsl -ldl -lm -lcrypt -lutil -lc
    libc=libc-2.24.so
    so=so
    useshrplib=false
    libperl=libperl.a
    gnulibc_version='2.24'
  Dynamic Linking:
    dlsrc=dl_dlopen.xs
    dlext=so
    d_dlsymun=undef
    ccdlflags='-Wl,-E'
    cccdlflags='-fPIC'
    lddlflags='-shared -O2 -g -L/usr/local/lib -fstack-protector-strong'

Locally applied patches:
    Devel::PatchPerl 1.46

---
@INC for perl 5.25.9:
    /home/jd/perl5/perlbrew/perls/perl-blead-new/lib/site_perl/5.25.9/x86_64-linux
    /home/jd/perl5/perlbrew/perls/perl-blead-new/lib/site_perl/5.25.9
    /home/jd/perl5/perlbrew/perls/perl-blead-new/lib/5.25.9/x86_64-linux
    /home/jd/perl5/perlbrew/perls/perl-blead-new/lib/5.25.9

---
Environment for perl 5.25.9:
    HOME=/home/jd
    LANG=en_US.UTF-8
    LANGUAGE (unset)
    LD_LIBRARY_PATH (unset)
    LOGDIR (unset)
    PATH=/home/jd/perl5/perlbrew/bin:/home/jd/perl5/perlbrew/perls/perl-blead-new/bin:/home/jd/.gems/bin:/home/jd/bin:/home/jd/bin:/usr/local
    PERLBREW_BASHRC_VERSION=0.76
    PERLBREW_HOME=/home/jd/.perlbrew
    PERLBREW_MANPATH=/home/jd/perl5/perlbrew/perls/perl-blead-new/man
    PERLBREW_PATH=/home/jd/perl5/perlbrew/bin:/home/jd/perl5/perlbrew/perls/perl-blead-new/bin
    PERLBREW_PERL=perl-blead-new
    PERLBREW_ROOT=/home/jd/perl5/perlbrew
    PERLBREW_VERSION=0.78
    PERL_BADLANG (unset)
    SHELL=/bin/bash
```

Thread Previous

- Re: [perl #130635] [PATCH] Stack overflow in Storable retrieve_hook by John Lightsey
- [perl #130635] [PATCH] Stack overflow in Storable retrieve_hook by James E Keenan via RT
- Re: [perl #130635] [PATCH] Stack overflow in Storable retrieve_hook by John Lightsey
- [perl #130635] [PATCH] Stack overflow in Storable retrieve_hook by James E Keenan via RT
- Re: [perl #130635] [PATCH] Stack overflow in Storable retrieve_hook by John Lightsey
- Re: [perl #130635] [PATCH] Stack overflow in Storable retrieve_hook by John Lightsey
- [perl #130635] [PATCH] Stack overflow in Storable retrieve_hook by James E Keenan via RT
- [perl #130635] [PATCH] Stack overflow in Storable retrieve_hook by James E Keenan via RT
- [perl #130635] [PATCH] Stack overflow in Storable retrieve_hook by James E Keenan via RT
- [perl #130635] [PATCH] Stack overflow in Storable retrieve_hook by James E Keenan via RT
- [perl #130635] [PATCH] Stack overflow in Storable retrieve_hook by James E Keenan via RT
- **[perl #130635] [PATCH] Stack overflow in Storable retrieve_hook** by John Lightsey

---